WHAT IS CLAIMED IS:

1. In a system for performing encryption communications using a common key updated at a predetermined timing between a key transmitting device and a key receiving device, a common key encryption communication system comprising:

a key transmitting device including first retaining unit retaining a most-updated encryption key and a one-generation-anterior encryption key as the above common keys, and first setting unit setting a one-generation-anterior encryption key for transmission and a most-updated encryption key and a one-generation-anterior encryption key for receipt, respectively; and

the above key receiving device including second retaining unit retaining a most-updated encryption key and a one-generation-anterior encryption key as the above common keys, and second setting unit setting a most-updated encryption key for transmission, and a most-updated encryption key and a one-generation-anterior key for receipt, respectively.

2. A common key encryption communication system according to claim 1, wherein the above key transmitting device further includes acquisition unit acquiring the encryption key, the above first retaining unit updates and retains the above most-updated encryption key as the

one-generation-anterior encryption key and the encryption key acquired by the above acquisition unit as the most-updated encryption key, respectively, and the above first setting unit re-sets the one-generation-anterior encryption key for transmission, and the most-updated encryption key and the one-generation-anterior encryption key for receipt respectively on the basis of the retained key after being updated by the above first retaining unit.

3. A common key encryption communication system according to claim 2, wherein the above key transmitting device includes generation unit generating the encryption key, and the above acquisition unit acquires the encryption key generated by the above generation unit.

4. A common key encryption communication system according to claim 2, wherein the above key transmitting device further includes first transmitting unit transmitting the encryption key acquired by the above acquisition unit to the key receiving device.

5. A common key encryption communication system according to claim 4, wherein the above key receiving device further includes second receiving unit receiving the encryption key transmitted from the above key transmitting device, in case the above second receiving

unit receives the encryption key, the above second retaining unit respectively updates and retains the above most-updated encryption key as the one-generation-anterior encryption key and the encryption key received by the above second receiving unit as the most-updated encryption key, and the above second setting unit respectively re-sets the most-updated encryption key for transmission, and the most-updated encryption key and the one-generation-anterior encryption key for receipt on the basis of the retained key after being updated by the above second retaining unit.

6. A common key encryption communication system according to claim 1, wherein the above key receiving device includes second transmitting unit transmitting a predetermined message to the key transmitting device, and the above key transmitting device includes first receiving unit receiving the predetermined message transmitted from the above key receiving device.

7. A common key encryption communication system according to claim 4, wherein the above first and second retaining unit respectively retain the initialization key.

8. A common key encryption communication system according to claim 7, wherein the above key receiving

device transmits a key initialization request message as the above predetermined message at a predetermined timing, in case the above key transmitting device receives the key initialization request message transmitted from the above key receiving device, the above acquisition unit acquires the encryption key, and the above first retaining unit respectively updates and retains the common initialization key as the one-generation-anterior encryption key and the encryption key acquired by the above acquisition unit as the most-updated encryption key.

9. A common key encryption communication system according to claim 4, wherein the above key receiving device transmits a key update request message as the above predetermined message at a predetermined timing, in case the above key transmitting device receives a key update request message transmitted from the above key receiving device, the above acquisition unit acquires the encryption key, and the above first retaining unit respectively updates and retains the above common initialization key as the one-generation-anterior encryption key and the encryption key acquired by the above acquisition unit as the most-updated encryption key.

10. A common key encryption communication system according to claim 9, wherein the above key receiving device includes unit determining a key update timing, and

said second transmitting unit, in the case of reaching the key update timing, transmits the key update request message to the key transmitting device.

11. A common key encryption communication system according to claim 4, wherein the above key transmitting device includes unit determining a key update timing, and said first transmitting unit, in the case of reaching the key update timing, transmits the encryption key acquired by the above acquisition unit to the key receiving device.

12. A common key encryption communication system according to claim 4, wherein the above key receiving device transmits a key resending request message as the above predetermined message at a predetermined timing, and, in case the above key transmitting device receives a key resending request message transmitted from the above key receiving device, the first transmitting unit transmits the encryption key acquired by the above acquisition unit to the key receiving device.

13. A common key encryption communication system according to claim 4, wherein the above first transmitting unit, in a state where the above first and second retaining unit retain none of the keys, transmits the encryption key acquired by the above acquisition unit to the key receiving device.

14. In a key transmitting device performing encryption communications using a common key updated at a predetermined timing with a key receiving device, a key transmitting device comprising retaining unit retaining a most-updated encryption key and a one-generation-anterior encryption key as the above common keys, and setting unit respectively setting a one-generation-anterior encryption key for transmission, and a most-updated encryption key and a one-generation-anterior encryption key for receipt.

15. In a key receiving device performing encryption communications using a common key updated at a predetermined timing with a key transmitting device, a key receiving device comprising retaining unit retaining a most-updated encryption key and a one-generation-anterior encryption key as the above common keys, and setting unit respectively setting a most-updated encryption key for transmission, and a most-updated encryption key and a one-generation-anterior encryption key for receipt.

16. In a method of performing encryption communications using a common key updated at a predetermined timing between a key transmitting device and a key receiving device, a common key encryption

communication method characterized in that the key transmitting device retains a most-updated encryption key and a one-generation-anterior encryption key as the above common keys, sets respectively the one-generation-anterior encryption key for transmission and for receipt, and the above key receiving device retains the most-updated encryption key and the one-generation-anterior encryption key as the above common keys, and sets respectively the most-updated encryption key for transmission and the most-updated encryption key and the one-generation-anterior encryption key for receipt.